BANGKO SENTRAL NG PILIPINAS

OFFICE OF THE GOVERNOR

CIRCULAR NO. 950
Series of 2017

Subject: **Amendments to Part Eight or the Anti-Money Laundering Regulations of the Manual of Regulations for Banks and Manual of Regulations for Non-Bank Financial Institutions**

By the authority vested to the Bangko Sentral ng Pilipinas to issue guidelines and circulars on anti-money laundering (AML) and combating the financing of terrorism (CFT), in order to effectively implement the provisions of Republic Act (R.A.) No. 9160, otherwise known as the "Anti-Money Laundering Act of 2001" (AMLA), as amended by R.A. Nos. 9194, 10167 and 10365, as provided under Rule 18 of the Revised Implementing Rules and Regulations (RIRR) of the AMLA, as amended, as well as R.A. No. 10168 or The Terrorism Financing Prevention and Suppression Act of 2012, as provided under Rule 27 of its Implementing Rules and Regulations (IRR), the Monetary Board, in its Resolution No. 334 dated 23 February 2017, approved the following amendments to Part Eight or the Anti-Money Laundering Regulations of the Manual of Regulations for Banks (MORB) and Manual of Regulations for Non-Bank Financial Institutions (MORNBFI).

Section 1. Sections X801/4801Q and X802/4802Q shall be amended to read, as follows:

"**Section X801/4801Q Declaration of Policy**. The Bangko Sentral adopts the policies of the State to (a) protect the integrity and confidentiality of bank accounts and ensure that the Philippines, in general, and the covered persons, in particular, shall not be used, respectively, as a money laundering site and conduit for the proceeds of an unlawful activity as herein defined; and (b) to protect life, liberty and property from acts of terrorism and to condemn terrorism and those who support and finance it and reinforce the fight against terrorism by criminalizing the financing of terrorism and related offenses."

"**Section X802/4802Q Scope of Regulations**. These regulations shall apply to all covered persons supervised and regulated by the Bangko Sentral. The term "*covered persons*" shall refer to banks, non-banks, QBs, trust entities, non-stock savings and loan associations, pawnshops, foreign exchange dealers, money changers, remittance and transfer companies, electronic money issuers and other financial institutions which under special laws are subject to Bangko Sentral supervision and/or regulation, including their subsidiaries and affiliates, which are

also covered persons, wherever they may be located. For this purpose, subsidiary and affiliate shall be defined as:

a. A *subsidiary* means an entity more than fifty percent (50%) of the outstanding voting stock of which is owned by a covered person.
b. An *affiliate* means an entity the voting stock of which, at least twenty percent (20%) to not more than fifty percent (50%), is owned by a covered person.

Pursuant to xxx

Whenever a covered person's branch, office, subsidiary or affiliate based outside the Philippines is prohibited from implementing this Part or any of the provisions of the AMLA, as amended, or its RIRR, by reason of local laws, regulations or a supervisory directive, said branch, office, subsidiary or affiliate, or the covered person shall (1) formally notify the Bangko Sentral of this situation and furnish a copy of the applicable laws and/or regulations or the supervising authority's directive, as the case may be; and (2) apply appropriate additional measures or mitigating controls to manage the money laundering (ML) and terrorist financing (TF) risks."

Section 2. Section X803/4803Q shall be amended to read as follows:

"Section X803/4803Q Definition of Terms. xxx

a. *Money laundering* is committed by any person who, knowing that any monetary instrument or property represents, involves, or relates to the proceeds of any unlawful activity:

    (1) transacts said monetary instrument or property;
    (2) converts, transfers, disposes of, moves, acquires, possesses or uses said monetary instrument or property;
    (3) conceals or disguises the true nature, source, location, disposition, movement or ownership of or rights with respect to said monetary instrument or property;
    (4) attempts or conspires to commit money laundering offenses referred to in Items *"(1)", "(2)" or "(3)"* above;
    (5) aids, abets, assists in or counsels the commission of the money laundering offenses referred to in Items *"(1)", "(2)" or "(3)"*above; and
    (6) performs or fails to perform any act as a result of which he facilitates the offense of money laundering referred to in Items *"(1)", "(2)" or "(3)"* above.

    Money laundering is also committed by any covered person who, knowing that a covered or suspicious transaction is required to be reported to the Anti-Money Laundering Council (AMLC) under any of the provisions of the AMLA, as amended, its RIRR, or this Part, fails to do so.

b. *Financing of terrorism* is a crime committed by a person who, directly or indirectly, willfully and without lawful excuse, possesses, provides, collects or uses property or funds or makes available property, funds or financial service or other related services, by any means, with the unlawful and willful intention that they should be used or with the knowledge that they are to be used, in full or in part: (1) to carry out or facilitate the commission of any terrorist act; (2) by a terrorist organization, association or group; or (3) by an individual terrorist.

c. *Covered transaction* (CT) refers to a transaction in cash or other equivalent monetary instrument exceeding five hundred thousand pesos (P500,000).

d. *Suspicious transaction* (ST) refers to a transaction with a covered person, regardless of the amount involved, where any of the following circumstances exists:

(1) There is no underlying legal or trade obligation, purpose or economic justification;
(2) The client is not properly identified;
(3) The amount involved is not commensurate with the business or financial capacity of the client;
(4) Taking into account all known circumstances, it may be perceived that the client's transaction is structured in order to avoid being the subject of reporting requirements under the AMLA, as amended;
(5) Any circumstance relating to the transaction which is observed to deviate from the profile of the client and/or the client's past transactions with the covered person;
(6) The transaction is in any way related to an unlawful activity or any money laundering activity or offense, that is about to be committed, is being or has been committed; or
(7) Any transaction that is similar, analogous or identical to any of the foregoing.

Any unsuccessful attempt to transact with a covered person, the denial of which is based on any of the foregoing circumstances, shall likewise be considered as suspicious transaction.

e. *Monetary instrument* shall include, but is not limited to the following:

(1) Coins or currency of legal tender of the Philippines, or of any other country;
(2) Credit instruments, including bank deposits, financial interest, royalties, commissions and other intangible property;
(3) Drafts, checks, and notes;
(4) Stocks or shares, participation or interest in a corporation or in a commercial enterprise or profit-making venture and evidenced by a certificate, contract, instrument, whether written or electronic in character including those enumerated in Section 3 of the Securities Regulation Code;

(5) A participation or interest in any non-stock, non-profit corporation;
(6) Securities or negotiable instruments, bonds, commercial papers, deposit certificates, trust certificates, custodial receipts or deposit substitute instruments, trading orders, transaction tickets and confirmations of sale or investments and money market instruments;
(7) Contracts or policies of insurance, life or non-life, contracts of suretyship, pre-need plans and member certificates issued by mutual benefit association; and
(8) Other similar instruments where title thereto passes to another by endorsement, assignment or delivery.

f. *Unlawful activity* refers to any act or omission or series or combination thereof involving or having direct relation to the following:

(1) xxx
(2) Sections 4, 5, 6, 8, 9, 10, 11, 12, 13, 14, 15, and 16 of R.A. No. 9165, otherwise known as the Comprehensive Dangerous Drugs Act of 2002;
(3) xxx
(4) xxx
(5) xxx
(6) xxx
(7) xxx
(8) xxx
(9) Swindling under Article 315 and "Other Forms of Swindling" under Article 316 of the RPC, as amended;
(10) Smuggling under R.A. Nos. 455 and 1937, as amended, otherwise known as the Tariff and Customs Code of the Philippines;
(11) xxx
(12) Hijacking and other violations under R.A. No. 6235, otherwise known as the "Anti-Hijacking Law"; "Destructive Arson"; and "Murder", as defined under the RPC, as amended;
(13) Terrorism and conspiracy to commit terrorism as defined and penalized under Sections 3 and 4 of R.A. No. 9372;
(14) Financing of terrorism under Section 4 and offenses punishable under Sections 5, 6, 7 and 8 of R.A. No. 10168, otherwise known as the Terrorism Financing Prevention and Suppression Act of 2012;
(15) Bribery under Articles 210, 211 and 211-a of the RPC, as amended, and Corruption of Public Officers under Article 212 of the RPC, as amended;
(16) Frauds and illegal exactions and transactions under Articles 213, 214, 215 and 216 of the RPC, as amended;
(17) Malversation of public funds and property under Articles 217 and 222 of the RPC, as amended;
(18) Forgeries and counterfeiting under Articles 163, 166, 167, 168, 169 and 176 of the RPC, as amended;
(19) Violations of Sections 4 to 6 of R.A. No. 9208, otherwise known as the Anti-trafficking in Persons Act of 2003, as amended;

(20) Violations of Sections 78 to 79 of Chapter IV, of Presidential Decree No. 705, otherwise known as the Revised Forestry Code of the Philippines, as amended;
(21) Violations of Sections 86 to 106 of Chapter IV, of R.A. No. 8550, otherwise known as the Philippine Fisheries Code of 1998;
(22) Violations of Sections 101 to 107, and 110 of R.A. No. 7942, otherwise known as the Philippine Mining Act of 1995;
(23) Violations of Section 27(C), (E), (F), (G) and (I), of R.A. No. 9147, otherwise known as the Wildlife Resources Conservation and Protection Act;
(24) Violation of Section 7(B) of R.A. No. 9072, otherwise known as the National Caves and Cave Resources Management Protection Act;
(25) Violation of R.A. No. 6539, otherwise known as the Anti-Carnapping Act of 2002, as amended;
(26) Violations of Sections 1, 3 and 5 of P.D. No. 1866, as amended, otherwise known as the Decree Codifying the Laws on Illegal/unlawful Possession, Manufacture, Dealing in, Acquisition or Disposition of Firearms, Ammunition or Explosives;
(27) Violation of P.D. No. 1612, otherwise known as the Anti-Fencing Law;
(28) Violation of Section 6 of R.A. No. 8042, otherwise known as the Migrant Workers and Overseas Filipinos Act of 1995, as amended by R.A. No. 10022;
(29) Violation of R.A. No. 8293, otherwise known as the Intellectual Property Code of the Philippines, as amended;
(30) Violation of Section 4 of R.A. No. 9995, otherwise known as the Anti-photo and Video Voyeurism Act of 2009;
(31) Violation of Section 4 of R.A. No. 9775, otherwise known as the Anti-child Pornography Act of 2009;
(32) Violations of Sections 5, 7, 8, 9, 10(C), (D) and (E), 11, 12 and 14 of R.A. No. 7610, otherwise known as the Special Protection of Children against Abuse, Exploitation and Discrimination;
(33) Fraudulent practices and other violations under R.A. No. 8799, otherwise known as the Securities Regulation Code of 2000; and
(34) Felonies or offenses of a nature similar to the aforementioned unlawful activities that are punishable under the penal laws of other countries.

In determining whether or not a felony or offense punishable under the penal laws of other countries is "of similar nature", as to constitute an unlawful activity under the AMLA, the nomenclature of said felony or offense need not be identical to any of the unlawful activities listed above.

g. *Transaction* refers to any act establishing any right or obligation or giving rise to any contractual or legal relationship between the parties thereto. It also includes any movement of funds by any means with a covered person.

h. *Proceeds* refers to an amount derived or realized from any unlawful activity.

i. *Monetary instrument or property related to an unlawful activity* refers to:

(1) All proceeds of an unlawful activity;
(2) All monetary, financial or economic means, devices, accounts, documents, papers, items or things used in or having any relation to any unlawful activity;
(3) All moneys, expenditures, payments, disbursements, costs, outlays, charges, accounts, refunds and other similar items for the financing, operations, and maintenance of any unlawful activity; and
(4) For purposes of freeze order and bank inquiry: related and materially-linked accounts.

(a) "Related accounts" refer to those accounts, the funds and sources of which originated from and/or are materially-linked to the monetary instruments or properties subject of the freeze order or an order of inquiry.

(b) "Materially-linked accounts" shall include the following:

(1) All accounts or monetary instruments under the name of the person whose accounts, monetary instruments, or properties are the subject of the freeze order or an order of inquiry;
(2) All accounts or monetary instruments held, owned, or controlled by the owner or holder of the accounts, monetary instruments, or properties subject of the freeze order or order of inquiry, whether such accounts are held, owned or controlled singly or jointly with another person;
(3) All "In Trust For" accounts where either the trustee or the trustor pertains to a person whose accounts, monetary instruments, or properties are the subject of the freeze order or order of inquiry;
(4) All accounts held for the benefit or in the interest of the person whose accounts, monetary instruments, or properties are the subject of the freeze order or order of inquiry; and
(5) All other accounts, shares, units, or monetary instruments that are similar, analogous, or identical to any of the foregoing.

j. *Client/Customer* refers to any person or entity who keeps an account, or otherwise transacts business with a covered person. It includes the following: (1) any person or entity on whose behalf an account is maintained or a transaction is conducted, as well as the beneficiary of said transactions; (2) beneficiary of a trust, an investment fund or a pension fund; (3) a company or person whose assets are managed by an asset manager; (4) a grantor of a trust; and (5) any insurance policy holder, whether actual or prospective.

k. *Shell company* refers to a legal entity which has no business substance in its own right but through which financial transactions may be conducted.

l. *Shell bank* refers to a shell company incorporated as a bank or made to appear to be incorporated as a bank but has no physical presence and no affiliation with a regulated financial group. It can also be a bank that (a) does not conduct business at a fixed address in a jurisdiction in which the shell bank is authorized to engage; (b) does not employ one or more individuals on a full time basis at this fixed address; (c) does not maintain operating records at this address, and (d) is not subject to inspection by the authority that licensed it to conduct banking activities.

m. *Beneficial owner* refers to any natural person(s) who ultimately owns or controls the customer and/or on whose behalf a transaction or activity is being conducted; or those who has ultimate effective control over a legal person or arrangement.

Ultimate effective control refers to situation in which ownership/control is exercised through actual or a chain of ownership or by means other than direct control.

n. *Politically exposed person or PEP* refers to an individual who is or has been entrusted with prominent public position in (1) the Philippines with substantial authority over policy, operations or the use or allocation of government-owned resources; (2) a foreign state, or (3) an international organization.

The term *PEP* shall include immediate family members, and close relationships and associates that are reputedly known to have:

(1) Joint beneficial ownership of a legal entity or legal arrangement with the main/principal PEP; or
(2) Sole beneficial ownership of a legal entity or legal arrangement that is known to exist for the benefit of the main/principal PEP.

Immediate family members of PEPs refer to spouse or partner, children and their spouses, and parents and parents-in-law;

Close associates of PEPs refer to persons who are widely and publicly known to maintain a particularly close relationship with the PEP, and include persons who are in a position to conduct substantial domestic and international financial transactions on behalf of the PEP.

o. *Correspondent banking* refers to the provision of banking services by one bank (the "correspondent bank") to another bank (the "respondent bank").

p. *Payable-through account* refers to a correspondent account that is used directly by third parties to transact business on their own behalf.

q. *Fund/wire transfer* refers to any transaction carried out on behalf of an originator (both natural and juridical) through an FI (originating institution) by electronic means with a view to making an amount of money available to a

beneficiary at another FI (beneficiary institution). The originator person and the beneficiary person may be the same person.

r. *Cross border* transfer refers to any wire transfer where the originating and beneficiary institutions are located in different countries. It shall also refer to any chain of wire transfer that has at least one cross border element.

s. *Domestic transfer* refers to any wire transfer where the originating and beneficiary institutions are located in the same country. It shall refer to any chain of wire transfers that takes place entirely within the borders of a single country, even though the system used to effect the fund/wire transfer may be located in another country.

t. *Originating institution* refers to the entity utilized by the originator to transfer funds to the beneficiary and can either be:

(1) a covered person as specifically defined by this Part and as generally defined by the AMLA, as amended, and its RIRR ; or
(2) An FI operating outside the Philippines that is other than the covered persons referred to in Item *"1"* but conducts business operations and activities similar to them.

u. *Beneficiary institution* refers to the entity that will pay out the money to the beneficiary and can either be:

(1) a covered person as specifically defined by this Part and as generally defined by the AMLA, as amended, and its RIRR ; or
(2) An FI operating outside the Philippines that is other than the covered persons referred to in Item *"1"* but conducts business operations and activities similar to them.

v. *Intermediary institution* refers to the entity utilized by the originating and beneficiary institutions where both have no correspondent banking relationship with each other but have established relationship with the intermediary institution. It can either be:

(1) a covered person as specifically defined by this Part and as generally defined by the AMLA, as amended, and its RIRR ; or
(2) An FI operating outside the Philippines that is other than the covered persons referred to in Item *"1"* but conducts business operations and activities similar to them.

w. *Official document* refers to any of the following identification documents:

(1) For Filipino citizens: Those issued by any of the following official authorities:
(a) Government of the Republic of the Philippines, including its political subdivisions, agencies, and instrumentalities;

(b) Government-Owned or -Controlled Corporations (GOCCs); or
(c) Covered persons registered with and supervised or regulated by the Bangko Sentral, SEC or IC;

(2) For foreign nationals: Passport or Alien Certificate of Registration;

(3) For Filipino students: School ID signed by the school principal or head of the educational institution; and

(4) For low risk customers: Any document or information reduced in writing which the covered person deems sufficient to establish the client's identity.

Section 3. Section X805/4805Q and its Subsections shall be amended to read as follows:

"**Section X805/4805Q Risk Management**. All covered persons shall develop sound risk management xxx to ensure that risks associated with ML/TF such as reputational, operational and compliance risks are xxx , to the end that covered persons shall not be used as a vehicle xxx.

The four (4) areas of xxx.

Subsection X805.1/4805Q.1 ***Board and senior management oversight.*** Notwithstanding xxx. For this reason, it shall ensure that oversight on the covered person's AML/CFT compliance management is adequate.

Senior management shall oversee the day-to-day management of the covered person, ensure effective implementation of AML/CFT policies approved by the board and alignment of activities with the strategic objectives, risk profile and corporate values set by the board. Senior management shall establish a management structure that promotes accountability and transparency and upholds checks and balances.

a. *Compliance Office.* Management of the implementation of the covered person's Money Laundering and Terrorist Financing Prevention Program (MLPP) shall be a primary task of the compliance office. To ensure the independence of the office, it shall have a direct reporting line to the board of directors or any board-level or approved committee on all matters related to AML and TF compliance and their risk management. It shall be principally responsible for the following functions among other functions that may be delegated by senior management and the board, to wit:

(1) Ensure compliance by all responsible officers and employees with this Part, the AMLA, as amended, the RIRR and its own MLPP. It shall conduct periodic compliance checking which covers, among others, evaluation of existing processes, policies and procedures including on-going monitoring of performance by staff and officers involved in ML and TF prevention,

reporting channels, effectiveness of the electronic money laundering transaction monitoring system and record retention system through sample testing and review of audit or examination reports. It shall also report compliance findings to the board or any board-level committee;

(2) Ensure that infractions, discovered either by internally initiated audits, or by special or regular examination conducted by the Bangko Sentral, or other applicable regulators, are immediately corrected;

(3) Inform all responsible officers and employees of all resolutions, circulars and other issuances by the Bangko Sentral and the AMLC in relation to matters aimed at preventing ML and TF;

(4) Alert senior management, the board of directors, or the board-level or approved committee if it believes that the covered person is failing to appropriately address AML/CFT issues; and

(5) Organize the timing and content of AML training of officers and employees including regular refresher trainings as stated in Section X809/4809Q.

b. Group-wide AML/CFT compliance. In case a covered person has branches, subsidiaries or offices located within and/or outside the Philippines, the group-wide compliance officer or in its absence, the compliance officer of the parent entity, shall oversee the AML/CFT compliance of the entire group with reasonable authority over the compliance officers of said branches, subsidiaries or offices.

Subsection X805.2/4805Q.2 ***Money laundering and terrorist financing prevention program (MLPP).*** All covered persons shall adopt a xxx. The MLPP shall be consistent with the AMLA, as amended, its RIRR and the provisions set out in this Part and designed according to the covered person's corporate structure and risk profile. It shall be in writing, xxx. Where a covered person has branches, subsidiaries, affiliates or offices located within and/or outside the Philippines, there shall be a consolidated ML/TF risk management system to ensure the coordination and implementation of policies and procedures on a group-wide basis, taking into account local business considerations and the requirements of the host jurisdiction.

The MLPP shall xxx. The covered person must put xxx:

a. Detailed procedures of the covered person's compliance and implementation of the following major requirements of the AMLA, as amended, its RIRR, and this Part, to wit:
   (1) xxx
   (2) xxx
   (3) xxx
   (4) Suspicious transaction (ST) reporting xxx. The ST reporting shall include a reporting chain under which a ST will be processed and the designation of a board-level or approved committee who will ultimately decide whether or not the covered person should file a report to the AMLC. If the resources of the covered person do not permit the designation of a committee, it may designate the compliance officer to perform this

function instead provided that the board of directors is informed of his decision.

b. An effective and continuous AML/CFT training program xxx;
c. xxx
d. xxx
e. xxx
f. A mechanism that ensures all deficiencies noted during the audit and/or Bangko Sentral regular or special examination or other applicable regulator's examination are immediately corrected and acted upon;
g. xxx;
h. Designation of an xxx. The AML compliance officer may also be the liaison between the covered person, the Bangko Sentral and the AMLC in matters relating to the covered person's AML/CFT compliance. Where resources of the covered person do not permit xxx; and
i. A mechanism where information required for customer due diligence and ML/TF risk management are accessible by the parent bank/entity and information are freely shared among branches, subsidiaries, affiliates and offices located within and/or outside the Philippines. Exchange of information among branches, subsidiaries, affiliates, and offices located within and/or outside the Philippines shall not be deemed a violation of Rule 9, Item C of the RIRR as long as this is done within the group. The MLPP may require a potential and/or existing customer to sign a waiver on the disclosure of information within the group.

Submission of the Revised and Updated MLPP. Approval by the Board of Directors or Country Head – Within six (6) months from effectivity of this Part, all covered persons shall prepare and have available for inspection an updated MLPP, approved by the board of directors, embodying the principles and provisions stated in this Part.

Henceforth, each MLPP shall be regularly updated at least once every two (2) years to incorporate changes in AML policies and procedures, latest trends in ML and TF typologies, and latest pertinent Bangko Sentral issuances. Any revision or update in the MLPP shall likewise be approved by board of directors or the country/regional head or its equivalent for local branches of foreign banks.

Subsection X805.3/4805Q.3 ***Monitoring and reporting tools.*** All covered persons shall adopt an AML/CFT monitoring system xxx. The system should be capable of generating timely, accurate and complete reports to lessen the likelihood of any reputational and compliance risks, and to regularly apprise the board of directors and senior management on AML/CFT compliance.

a. *Electronic monitoring and reporting systems for AML/CFT.* UBs and KBs and such covered persons that are considered complex pursuant to Subsec. X141.3/4141Q.3 shall adopt an electronic AML system capable of monitoring risks associated with ML/TF as well as generating timely reports for the guidance and information of its board of directors and senior

management, in addition to the functionalities mentioned in Subsec. X807.2/4807Q.2.

b. *Manual monitoring.* Covered persons not required to adopt an AML/CFT electronic system must ensure that they have the means of complying with Subsec. X805.3/4805Q.3.

Subsection X805.4/4805Q.4 *Internal audit.* The internal audit function xxx.

The Internal Audit shall xxx.

For covered persons with electronic AML/CFT transaction monitoring system, in addition to the above, the internal audit shall include determination of the efficiency of the system's functionalities as required by Subsecs. X805.3/4805Q.3 and X807.2/4807Q.2.

The results of the internal audit shall be timely communicated to the board of directors and shall be open for scrutiny by Bangko Sentral examiners xxx. Results of the audit shall likewise be promptly communicated to the Compliance Office for appropriate monitoring of corrective actions taken by the different business units concerned. The Compliance Office shall regularly submit reports to the board to inform them of management's action to address deficiencies noted in the audit.

Subsection X805.5/4805Q.5 *Risk assessment.* Consistent with risk-based approach, covered persons are required to identify, understand and assess their ML/TF risks, arising from customers, countries or geographic areas of operations and customers, products, services, transactions or delivery channels. The assessment methodology shall be appropriate to the nature of operations and complexity of the business of the covered person. The risk assessment shall (a) consider all relevant risk factors; (b) adequately document results and findings; and (c) be updated periodically or as necessary. Based on the risk assessment, the covered person shall take appropriate measures to manage and mitigate ML/TF risks. The risk assessment shall be made available to the Bangko Sentral during examination or in other circumstances deemed necessary as part of continuous supervision.

New products and business practices risk assessment. Covered persons are also required to identify and assess the ML/TF risks that may arise in relation to the development of new products and new business practices, including new delivery mechanisms, and the use of new or developing technologies for both new and pre-existing products. Such risk assessment should be an integral part of product or service development process and should take place prior to the launch of the new products, business practices or the use of new or developing technologies. Covered persons should take appropriate measures to manage and mitigate the identified risks."

Section 4. Section X806/4806Q and Subsections X806.1 to X806.1.d/4806Q.1 to 4806Q.1.d shall be amended to read as follows:

"Section X806/4806Q Customer Due Diligence.

a. In conducting customer due diligence, a risk-based approach shall be undertaken depending on the type of customer, business relationship or nature of the product, transaction or activity. In this regard, a covered person shall maintain a system that will ensure the conduct of customer due diligence which shall include:

   (1) Identifying the customer and verifying the true identity of the customer based on official documents or other reliable, independent source documents, data or information. In case of corporate and juridical entities, verifying their legal existence and organizational structure, as well as the authority and identification of all persons purporting to act on their behalf;
   (2) Identifying the beneficial owner and taking reasonable measures to verify the identity of the beneficial owner, such that the covered person shall be satisfied that it knows who the beneficial owner is, as well as the ownership and control structure of the customer, in case of juridical entities or legal arrangements;
   (3) Understanding and, as appropriate, obtaining information on the purpose and intended nature of the business relationship; and
   (4) Conducting ongoing due diligence on the business relationship and scrutiny of transactions undertaken throughout the course of the relationship to ensure that the transactions being conducted are consistent with the covered person's knowledge of the customer, their business and risk profile.

b. A covered person shall be required to undertake customer due diligence when:

   (1) It establishes business relations with any customer;
   (2) It undertakes any occasional but relevant business transaction for any customer who has not otherwise established relations with the covered person;
   (3) There is a suspicion of money laundering or terrorism financing; or
   (4) There is doubt about the veracity or adequacy of previously obtained customer identification data.

c. "Business relations" means the opening or maintenance of an account or the provision of financial advice by the covered person to a customer.

d. "Relevant business transaction" shall refer to:

   (1) A transaction with a value exceeding P100,000, except money changing or remittance transactions;

(2) Two or more transactions believed to be linked and with an aggregate value exceeding P100,000; or
(3) In relation to remittance and money changing transactions, any transaction or two or more transactions believed to be linked, with an aggregate value exceeding P5,000.00.

For this purpose, covered persons should have appropriate system to identify and determine occasional customer or transaction.

Subsection X806.1/4806Q.1 ***Customer acceptance and identification policy.*** Every covered person shall develop clear, written and graduated customer acceptance and identification policies and procedures that will ensure that the financially or socially disadvantaged are not denied access to financial services while at the same time prevent suspicious individuals or entities from opening an account or establishing a relationship. A covered person shall formulate a risk-based and tiered customer acceptance, identification and retention policy that involves reduced customer due diligence (CDD) for potentially low risk clients and enhanced CDD for higher risk accounts.

a. *Criteria for type of customers: low, normal and high risk; Standards for applying reduced, average and enhanced due diligence.* Covered persons shall specify the criteria and description of the types of customers that are likely to pose low, normal or high ML/TF risk to their operations, as well as the standards in applying reduced, average and enhanced due diligence, including a set of conditions for the denial of account opening or services.

   Enhanced due diligence shall be applied to customers that are assessed by the covered person or under this Part as high risk for ML/TF. For customers assessed to be of low risk such as small account balance and transactions, a covered person may apply reduced due diligence. Some entities may likewise be considered as low risk clients, e.g., banking institutions, trust entities and QBs authorized by the Bangko Sentral to operate as such and publicly listed companies subject to regulatory disclosure requirements.

   In designing a customer acceptance and risk profiling policy, the following criteria relating to the product or service, the customer, and geographical location, at a minimum, shall be taken into account:

   (1) The nature of the service or product to be availed of by the customers and the purpose of the account or transaction;
   (2) Source of funds/nature of business activities;
   (3) Public or high profile position of the customer or its directors/trustees, stockholders, officers and/or authorized signatory;
   (4) Country of origin and residence of operations or the fact that a customer came from a high risk jurisdiction;
   (5) The existence of suspicious transaction indicators;
   (6) Watchlist of individuals and entities engaged in illegal activities or terrorist-related activities as circularized by the Bangko Sentral, xxx; and

(7) Such other factors, e.g., the amount of funds to be deposited by a customer or the size of transactions, and regularity or duration of the transaction, as the covered person may deem reasonable or necessary to consider in assessing the risk of a customer to ML/TF.

In assessing the risk profile of customers which are juridical entities, the covered person should also consider the financial profile and other relevant information of the active authorized signatories.

The covered person shall document the risk profiling results as well as how a specific customer was profiled and what standard of CDD (reduced, average or enhanced) was applied.

b. *Enhanced due diligence (EDD).* Whenever EDD is applied as required by this Part, or by the covered person's customer acceptance policy, or where the risk of ML/TF are higher, the covered person shall do all of the following, in addition to profiling of customers and monitoring their transactions:

(1) Gather additional customer information and/or identification documents, other than the minimum information and/or documents required for the conduct of average due diligence as enumerated under Subsec. X806.2/ 4806Q.2:

(a) In case of individual customers - (i) supporting information on the intended nature of the business relationship/source of funds/ source of wealth (such as financial profile, ITR, Loan Application, Deed of Donation, Deed of Sale, etc.);(ii) reasons for intended or performed transactions; (iii) list of companies where he is a stockholder, director, officer, or authorized signatory; (iv) other relevant information available through public databases or internet; and (v) a list of banks where the individual has maintained or is maintaining an account.

(b) In case of entities - (i) prior or existing bank references; (ii) the name, present address, nationality, date of birth, nature of work, contact number and source of funds of each of the primary officers (e.g. President, Treasurer); (iii) volume of assets, other information available through public databases or internet and supporting information on the intended nature of the business relationship, source of funds or source of wealth of the customer (ITR, Audited Financial Statement, Loan Application, Deed of Donation, Deed of Sale, etc.); and (iv) reasons for intended or performed transactions.

(2) Conduct validation procedures in accordance with Subsec. X806.1(c)/ 4806Q.1(c) on any or all of the information provided;

(3) Secure senior management approval to commence or continue business relationship/transacting with the customer;

(4) Conduct enhanced ongoing monitoring of the business relationship, by, among others, increasing the number and timing of controls applied, and selecting patterns of transactions that need further examination;
(5) Require the first payment to be carried out through an account in the customer's name with a bank subject to similar CDD standards, where applicable; and
(6) Perform such other measures as the covered person may deem reasonable or necessary.

Where additional information cannot be obtained, or any information or document provided is false or falsified, or result of the validation process is unsatisfactory, the covered person shall deny banking relationship with the customer without prejudice to the reporting of a suspicious transaction to the AMLC when circumstances warrant.

c. *Minimum validation procedures for EDD.* The procedures performed must enable the covered person to achieve a reasonable confidence and assurance that the information obtained are true and reliable.

Validation procedures for individual customers shall include, but are not limited to, the following:

(1) Confirming the date of birth from a duly authenticated official document;
(2) Verifying the address through evaluation of utility bills, bank or credit card statement, sending thank you letters, or other documents showing address or through on-site visitation;
(3) Contacting the customer by phone or email;
(4) Determining the authenticity of the identification documents through validation of its issuance by requesting a certification from the issuing authority or by any other effective and reliable means; or
(5) Determining the veracity of the declared source of funds.

For corporate or juridical entities, verification procedures shall include, but are not limited to, the following:

(1) Validating source of funds or source of wealth from reliable documents such as audited financial statements, ITR, bank references, etc.;
(2) Inquiring from the supervising authority the status of the entity;
(3) Verifying the address through on-site visitation of the company, sending thank you letters, or other documents showing address; or
(4) Contacting the entity by phone or email.

d. *Reduced due diligence.* Where lower risks of ML/TF have been identified, through an adequate analysis of risk by the covered person, reduced due diligence procedures may be applied. The reduced due diligence procedures should be commensurate with the lower risk factors, but are not acceptable whenever there is suspicion of ML/TF, or specific higher risk scenarios apply.

Whenever reduced due diligence is applied as provided in this Part or in the covered person's customer acceptance policy, the following rules shall apply:

(1) For individual customers, a covered person may open an account/establish relationship under the true and full name of the account owner/s or customers upon presentation of an acceptable identification card (ID) or official document as defined in this Part or other reliable, independent source documents, data or information.
(2) For corporate, partnership, and sole proprietorship entities, a covered person may open an account under the official name of these entities by presenting a Board Resolution duly certified by the Corporate Secretary, or equivalent document, authorizing the signatory to sign on behalf of the entity, obtained at the time of account opening.

Verification of the identity of the customer, beneficial owner or authorized signatory can be made after the establishment of the business relationship.

e. *Restricted account*. To promote financial inclusion and to ensure that the micro-business owners and the low-income households are able to manage their finances through the financial system, customers who may not be able to provide any of the required information under Subsec. X806.2/4806Q.2 for valid reasons or any valid identification document (ID) under Subsec. X806.2 (c)/4806Q.2 (c) may be allowed to open a restricted account with a covered person, provided:

(1) the aggregate credits in a year shall not exceed P100,000; and
(2) the account shall not be allowed to receive/send foreign remittances.

In lieu of a valid ID, the covered person shall obtain the customer's complete name, birth date, source of funds, present and/or permanent address and nationality and ensure that it has in its records a clear photograph and signature or thumbprint of the customer.

The account opening shall be subject to the condition that the customer shall obtain a valid ID within twelve (12) months; otherwise the account shall be closed and the remaining balance therein shall be returned to the customer. An extension of another twelve (12) months may be allowed; *Provided*, That the customer is able to show to the covered person a proof of application for a valid ID.

The covered person shall ensure that the above conditions are not breached; otherwise complete information and valid ID shall immediately be required or the account shall be closed accordingly."

Section 5. Subsections X806.1.e to X806.1.e.3/4806Q.1.e to 4806Q.1.e.3 shall be deleted and its provisions incorporated in Subsection X806.2/4806Q.2 as provided in Section 6 below.

Section 6. Subsection X806.2/4806Q.2 shall be amended to read as follows:

"**Subsection X806.2/4806Q.2** ***Customer identification.*** Covered persons shall establish and verify the true identity of its customers based on official document as defined in this Part or other reliable, independent source documents, data or information.

a. New individual customers. Covered persons shall develop a systematic procedure for establishing the true and full identity of new individual customers, and shall open and maintain the account/relationship only in the true and full name of the account/relationship owner/s.

Unless otherwise stated in this Part, average customer due diligence requires that the covered person obtain from individual customers, at the time of account opening/establishing the relationship, the following minimum information and confirming these information with the official or valid identification documents:

(1) Name of customer;
(2) Date and place of birth;
(3) Name, present address, date and place of birth, nationality, nature of work and source of funds of beneficial owner, whenever applicable;
(4) Present address;
(5) Permanent address;
(6) Contact number or information;
(7) Nationality;
(8) Specimen signature or biometrics of the customer;
(9) Nature of work, name of employer or nature of self-employment/ business;
(10) Source/s of funds; and
(11) Tax identification number (TIN) and Social Security System (SSS) number or Government Service Insurance System (GSIS) number, as may be applicable.

b. New corporate and juridical entities. A covered person shall develop a systematic procedure for identifying corporate, partnership and sole proprietorship entities, as well as their stockholders/partners/owners, directors, officers and authorized signatories. It shall open and maintain accounts only in the true and full name of the entity and shall have primary responsibility to ensure that the entity has not been, or is not in the process of being dissolved, struck-off, wound-up, terminated or otherwise placed under receivership or liquidation.

Unless otherwise stated in this Part, average due diligence requires that the covered person obtain the following minimum information and/or documents before establishing business relationships:

(1) Customer information
   (a) Name of entity;
   (b) Name, present address, date and place of birth, nationality, nature of work and source of funds of beneficial owner or beneficiary, if applicable, and authorized signatories;
   (c) Official address;
   (d) Contact numbers or information;
   (e) Nature of business; and
   (f) Specimen signatures or biometrics of the authorized signatory.

(2) Identification Documents
   (a) Certificates of Registration issued by the Department of Trade and Industry (DTI) for single proprietors, or by the Securities and Exchange Commission for corporations and partnerships, and by the Bangko Sentral for money changers/foreign exchange dealers and remittance and transfer companies;
   (b) Secondary license or certificate of authority issued by the supervising authority or other government agency;
   (c) Articles of Incorporation/Partnership;
   (d) Latest General Information Sheet which lists the names of directors/trustees/partners, principal stockholders owning at least twenty percent (20%) of the outstanding capital stock and primary officers such as the President and Treasurer;
   (e) Board or Partners' resolution duly certified by the Corporate/ Partners' Secretary, or other equivalent document, authorizing the signatory to sign on behalf of the entity; and
   (f) For entities registered outside of the Philippines, similar documents and/or information shall be obtained duly authenticated by a senior officer or the designated officer of the covered person assigned in the country of registration; in the absence of said officer, the documents should be authenticated by the Philippine Consulate, company register or notary public, where said entities are registered.

For legal arrangement (e.g., Trust), the following must be obtained:

(1) Name of legal arrangement and proof of existence;
(2) Address and country of establishment;
(3) Nature, purpose and objects of the legal arrangement;
(4) The names of the settlor, the trustee, the trustor, the protector, if any, the beneficiary and any other natural person exercising ultimate effective control over the legal arrangement;
(5) Description of the purpose/activities of the legal arrangement;
(6) Expected use of the account; and
(7) Amount, number, type, purpose and frequency of the transaction expected.

c. *Valid identification documents.*

(1) Customers and the authorized signatory/ies of a corporate or juridical entity who engage in a financial transaction with a covered person for the first time shall be required to present official identification document which shall include any of the official documents as defined in this Part or other identification information which can be verified from reliable, independent source, documents, data or information, such as third-party verified customer information database.

(2) A covered person may classify identification documents based on its reliability and ability to validate the information indicated in the identification document with that provided by the customer. Whenever it deems necessary, a covered person may accept other IDs not provided herein: *Provided,* That it shall not be the sole means of identification.

In case the identification document presented does not bear any photo of the customer or authorized signatory, or the photo-bearing ID or a copy thereof does not clearly show the face of the customer or authorized signatory, a covered person may utilize its own technology to take the photo of the customer or authorized signatory.

Relief in case of calamity. In case of a disastrous calamity and subject to a declaration by the Bangko Sentral on the applicability of this relief, any requirement for the presentation of valid ID shall be relaxed, subject to the following conditions:

(1) The amount of transactions shall not exceed P50,000.00 per day;
(2) The customer is either a permanent or temporary resident or who conducts business in a severely affected area which has been declared to be under a state of calamity by a competent authority;
(3) The customer shall submit a written certification, which need not be notarized, that he/she is a victim of the subject disastrous calamity and has lost his/her valid IDs; and
(4) The customer's account activities shall be subject to strict monitoring by the covered person to identify potential abuse of the relaxed requirement and any suspicious transactions shall be reported to the AMLC within the prescribed period.

d. *Face-to-face contact.* Covered persons shall conduct face-to-face contact and personal interview at the commencement of the relationship, or as reasonably practicable so as not to interrupt the normal conduct of business, taking into account the nature of the product, type of business and the risks involved: *Provided,* That ML/TF risks are effectively managed.

The use of Information and Communication Technology (ICT) in the conduct of face-to-face contact and interview may be allowed: *Provided,* That the covered

person is in possession of and has verified the identification documents submitted by the prospective client prior to the interview and that the entire procedure is documented.

The covered person shall clearly define the instances when the conduct of face-to-face is reasonably practicable, depending on the product, type of business and risk involved, or when the use of ICT shall apply. Also, the covered person should adopt policies and procedures to address any specific risks associated with deferred or technology-aided face-to-face verification and personal interview.

e. *Outsourcing of the gathering of minimum information and/or documents and face-to-face contact.* Subject to existing rules on outsourcing of specified banking activities, a covered person may, without prior Monetary Board approval, outsource to a counterparty, which may or may not be a covered person as herein defined, the gathering of the minimum information and/or documents and face-to-face contact as required under this Part: *Provided*, That the ultimate responsibility for knowing the customer and for keeping the identification documents shall lie with the covered person and the following conditions are complied with:

For covered person counterparty:

(1) There is a written service level agreement approved by the board of directors of both covered persons; and
(2) The counterparty has a reliable and acceptable customer identification system and training program in place.

For non-covered person counterparty:

(1) All conditions required for covered person counterparty;
(2) The covered person outsourcing the activity shall ensure that the employees or representatives of the counterparty gathering the required information/documents of, and/or conducting face-to-face contact with, the customer undergo equivalent training program as that of the covered person's own employees undertaking a similar activity; and
(3) The covered person shall monitor and conduct annual review of the performance of the counterparty to determine whether or not to continue with the arrangement.

All identification information and/or documents shall be turned over within a period not exceeding ninety (90) calendar days to the covered person, which shall carefully review the documents or information and conduct the necessary risk assessment of the customer. The covered person may, however, include in the coverage of the outsourcing agreement the safekeeping of the documents gathered subject to the condition that customer identification documents shall be made available to the covered person or to the competent authorities within three (3) banking days from the date of request.

f. *Third party reliance.* A covered person may rely on the identification process or gathering of minimum information and face-to-face contact undertaken by a third party subject to the following rules:

(1) *Where the third party is a covered person specifically defined by this Part and as generally defined by AMLA, as amended, and its RIRR* - The covered person shall obtain from the third party a written sworn certification containing the following:

(a) The third party has conducted the prescribed customer identification procedures in accordance with this Part and its own MLPP, including the face-to-face contact requirement, to establish the existence of the ultimate customer and has in its custody all the minimum information and/or documents required to be obtained from the customer; and
(b) The relying covered person shall have the ability to obtain identification documents from the third party upon request without delay.

(2) *Where the third party is a financial institution operating outside the Philippines that is other than covered persons referred to in* Item *"1" above but conducts business operations and activities similar to them* - All the contents required in the sworn certification mentioned in Item "*1*" above shall apply, with the additional requirement that the laws of the country where the third party is operating has equal or more stringent customer identification process requirement and that it has not been cited in violation thereof. It shall, in addition to performing normal due diligence measures, do the following:

(a) Gather sufficient information about the third party and the group to which it belongs to understand fully the nature of its business and determine from publicly available information the reputation of the institution and the quality of supervision, including whether or not it has been subject to ML or TF investigation or regulatory action;
(b) Document the respective responsibilities of each institution; and
(c) Obtain approval from senior management at inception of relationship before relying on the third party.

A Bangko Sentral-accredited custodian may likewise rely, in accordance with this Part, on the face-to-face contact and gathering of minimum information performed by the seller or issuer of securities or by the global custodian to establish the existence and full identity of the customer: *Provided*, That the said third party has an equivalent customer identification requirements.

Notwithstanding the foregoing, the ultimate responsibility for identifying the customer still lies with the covered person relying on the third party.

In cases where the customer is assessed as high risk by the third party, the covered person shall conduct its separate enhanced due diligence procedure.

g. *Trustee, nominee, agent or intermediary account.* Where (1) an account is opened by; (2) relationship is established through, or (3) any transaction is conducted by, a trustee, nominee, agent or intermediary, either as an individual or through a fiduciary relationship or similar arrangements, the covered person shall establish and record the true and full identity and existence of both the (1) trustee, nominee, agent or intermediary; and (2) trustor, principal, beneficial owner or person on whose behalf the account/relationship/transaction is being opened/established/conducted. The covered person shall determine the true nature of the parties' capacities and duties by obtaining a copy of the written document evidencing their relationship and apply the same standards for assessing the risk profile and determining the standard of due diligence to be applied to both.

In case of several trustors, principals, beneficial owners, or persons on whose behalf the account is being opened/relationship is being established, where the trustee, nominee, agent or intermediary opens a single account but keeps therein sub-accounts that may be attributable to each trustor, principal, or beneficial owner, the covered person shall, at the minimum, obtain the true and full name, place and date of birth or date of registration, as the case may be, present address, nature of work or business and source of funds as if the account was opened by them separately. Where the covered person is required to report a CT or circumstances warrant the filing of an ST, it shall obtain such information on every trustor, principal, beneficial owner, or person on whose behalf the account is being opened in order that a complete and accurate report may be filed with the AMLC.

In case a covered person entertains doubts as to whether the trustee, nominee, agent, or intermediary is being used as a dummy in circumvention of existing laws, it shall apply enhanced due diligence in accordance with Subsec. X806.1 (b)/4806Q.1 (b) and file a suspicious transaction report, if warranted.

h. *Private banking/wealth management operations.* These services, which by their nature involve high measure of client confidentiality, are more open to the elements of reputational risk especially if the customer identification process is not diligently followed. Covered persons shall therefore establish and record the true and full identify and take reasonable measures to establish the source of wealth and source of funds, of the customer and beneficial owners, if any, and establish a policy on what standard of due diligence will apply to them. They shall also require approval by a senior officer other than the private banking/ wealth management/similar activity relationship officer or the like for acceptance of customers of private banking, wealth management and similar activities.

i. *Politically exposed person (PEP).* Covered persons shall establish and record the true and full identity of PEPs, as well as their immediate family members and entities related to them.

(1) In case of domestic PEPs or persons who have been entrusted with a prominent function by an international organization, or their immediate family members or close associates, in addition to performing the applicable due diligence measures, covered persons shall:

(a) Take reasonable measures to determine whether a customer or the beneficial owner is a PEP; and
(b) In cases when there is a higher risk business relationship, adopt measures under paragraphs (2)(b) to (2) (d) below.

(2) In relation to foreign PEPs or their immediate family members or close associates, in addition to performing the applicable customer due diligence measures, covered persons shall:

(a) Put in place risk management systems to determine whether a customer or the beneficial owner is a PEP;
(b) Obtain senior management approval before establishing (or continuing, for existing customers) such business relationship;
(c) Take reasonable measures to establish the source of wealth and the source of funds of customers and beneficial owners identified as PEPs; and
(d) Conduct enhanced ongoing monitoring on that relationship.

j. Correspondent banking. Covered persons shall adopt policies and procedures to prevent correspondent banking activities from being utilized for ML/TF activities, and designate an officer responsible in ensuring compliance with these regulations and the covered person's policies and procedures.

A covered person may rely on the customer identification process undertaken by the respondent bank and apply the rules on third party reliance under Subsec. X806.2 (f)/4806Q.2 (f), treating the respondent bank as the third party. The correspondent bank shall:

(1) In relation to cross border correspondent banking and other similar relationship -

(a) Gather sufficient information about the respondent institution to understand fully the nature of the respondent's business, and to determine from publicly available information the reputation of the institution and the quality of supervision, including whether it has been subject to ML/TF investigation or regulatory action;
(b) Assess the respondent institution's AML/CFT controls;
(c) Obtain approval from senior management before establishing new correspondent relationships; and

(d) Clearly understand and document the respective AML/CFT responsibilities of each institution.

(2) With respect to *"payable-through accounts,"* satisfy themselves that the respondent bank:

(a) Has performed customer due diligence obligations on its customers that have direct access to the accounts of the correspondent bank; and
(b) Is able to provide relevant customer due diligence information upon request to the correspondent bank.

Covered persons are prohibited from entering into, or continuing, correspondent banking relationships with shell banks and should have measures to satisfy themselves that respondent financial institutions do not permit their accounts to be used by shell banks.

k. *Fund/Wire transfer.* Because of the risk associated with dealing with fund/wire transfers, where a covered person may unknowingly transmit proceeds of unlawful activities or funds intended to finance terrorist activities, it shall establish policies and procedures designed to prevent it from being utilized for that purpose which shall include, but not limited to, the following:

(1) The beneficiary institution shall not accept instructions to pay-out fund transfers to non-customer beneficiary, unless it has conducted the necessary customer due diligence to establish the true and full identity and existence of said beneficiary. Should the originator and beneficiary be the same person, the beneficiary institution may rely on the customer due diligence conducted by the originating institution provided the rules on third party reliance under Subsection X806.2 (f)/4806Q.2 (f) are met, treating the originating institution as third party as therein defined;
(2) The originating institution shall not accept instructions to fund/wire transfer from a non-customer originator, unless it has conducted the necessary customer due diligence to establish the true and full identity and existence of said originator;
(3) In cross border transfers, if the originator is a high risk customer as herein described, the beneficiary institution shall conduct enhanced due diligence on the beneficiary and the originator. Where additional information cannot be obtained, or any information or document provided is false or falsified, or result of the validation process is unsatisfactory, the beneficiary institution shall refuse to effect the fund/wire transfer or the pay-out of funds without prejudice to the reporting of a suspicious transaction to the AMLC when circumstances warrant;
(4) Whenever possible, manually initiated funds transfer (MIFT) instructions should not be the primary delivery method. Every effort shall be made to provide client with an electronic banking solution. Where MIFT is utilized, the following validation procedures shall apply:

(i) Prior to the bank accepting from a customer a manually initiated funds transfer request, the customer must execute and sign an agreement which preferably is part of the account opening documentation, wherein are outlined the manual instruction procedures with related security procedures including customer agreement to accept responsibility for fraudulent or erroneous instructions provided the bank has complied with the stated security procedures.

(ii) It is mandatory that written MIFT instructions are signature verified. In addition, one (1) of the following primary security procedures must be applied: a recorded callback to the customer to confirm the transaction instructions, or testword arrangement/ verification. The callback or test word requirement may be substituted by any of the following validity checks: use of a controlled PIN or other pre-established code; sequential numbering control of messages; pre-established verifiable forms; same as prior transmissions; standing/predefined instructions; or value for value transactions.

(iii) It is mandatory that MIFT instructions are signature verified and the device be located in a secured environment with limited and controlled staff access which permits visual monitoring. If monitoring is not possible, the device must be secured or programmed to receive messages into a password protected memory.

MIFT transactions below a certain threshold (approved by the President/Country Manager (for branches of foreign banks) or Business Risk Manager) may be processed with the mandatory procedure described above and an enhanced security procedure such as (a) a recorded callback to the customer to confirm the transaction instructions and/or (b) test word arrangement/verification, and/or (c) utilization of secured forms that incorporate verifiable security procedures such as watermarks or codes, and/or (d) transmission encryption.

(iv) Telephone callback numbers and contacts must be securely controlled. The confirmation callback is to be recorded and made to the signatory/(ies) of the customer's individual account(s). For commercial and company accounts the callback will be made to the signatory/(ies) of the account or, if so authorized, another person designated by the customer in the MIFT agreement. The party called is to be documented on the instructions. The callback must be made by someone other than (a) the person receiving the original instructions and (b) effecting the signature verification.

(5) Cross border and domestic fund/wire transfers and related message not exceeding P50,000.00 or its equivalent in foreign currency, shall include accurate and meaningful originator and beneficiary information. The following information shall remain with the transfer or related message through the payment chain:

(a) Name of the originator;

(b) Name of the beneficiary; and
(c) Account number of the originator and beneficiary, or in its absence, a unique reference number.

(6) For cross border and domestic fund/wire transfers and related message amounting to ₱50,000.00 or more, or its equivalent in foreign currency, the following information shall be obtained and accompany the wire transfer:

(a) Name of the originator;
(b) Originator account number where such an account is used to process the transaction or a unique transaction reference number which permits traceability of the transaction;
(c) Originator's address, or national identity number, or customer identification number, or date and place of birth;
(d) Name of the beneficiary; and
(e) Beneficiary account number where such an account is used to process the transaction, or unique transaction reference number which permits traceability of the transaction.

For domestic wire transfers, the originating institution should ensure that the required information accompanies the wire transfers, unless this information can be made available to the beneficiary institution and relevant authorities by other effective means. In the latter case, the ordering institution shall include only the account number or a unique identifier within the message or payment form which will allow the transaction to be traced back to the originator or beneficiary. Originating institutions are required to provide the information within three (3) working days from receiving the request either from the beneficiary institution or from relevant authorities or agencies.

(7) Should any wire/fund transfer amounting to P50,000.00 or more or its equivalent be unaccompanied by the required originator information, the beneficiary institution shall exert all efforts to establish the true and full identity and existence of the originator by requiring additional information from the originating institution or intermediary institution. It shall likewise apply enhanced due diligence to establish the true and full identity and existence of the beneficiary. Where additional information cannot be obtained, or any information or document provided is false or falsified, or result of the validation process is unsatisfactory, the beneficiary institution shall refuse to effect the fund/wire transfer or the pay-out of funds without prejudice to the reporting of a suspicious transaction to the AMLC when circumstances warrant.

l. Buyers of cashier's, manager's or certified checks. A covered person may sell cashier's, manager's or certified checks only to its existing customers and shall maintain a register of said checks indicating the following information:

(1) True and full name of the buyer or the applicant if buying on behalf of an entity;
(2) Account number;
(3) Date of issuance and the number of the check;
(4) Name of the payee;
(5) Amount; and
(6) Purpose of such transaction.

(a) *Buyers of cashier's, manager's or certified checks other than its existing customer.* Where an individual or an entity other than an existing customer applies for the issuance of cashier's, manager's or certified checks, the covered person shall, in addition to the information required in Subsec X806.2 (I)/4806Q.2 (I), obtain all the identification documents and minimum information required under this Part to establish the true and full identity and existence of the applicant. In no case shall reduced due diligence be applied to the applicant and, where circumstances warrant, enhanced due diligence should be applied.

(b) *Buyers of cashier's, manager's or certified checks in blank or payable to cash, bearer or numbered account.* A covered person may issue cashier's, manager's or certified checks or other similar instruments in blank or payable to cash, bearer or numbered account subject to the following conditions:

(i) The amount of each check shall not exceed P10,000;
(ii) The buyer of the check is properly identified in accordance with its customer acceptance and identification policies and as required under Subsec. X806.2 (I) /4806Q.2 (I) and Subsec. X806.2 (I) (a) /4806Q.2 (I) (a);
(iii) A register of said checks indicating all the information required under Subsec. X806.2 (I)/4806Q.2 (I);
(iv) A covered person which issues as well as those which accepts as deposits, said cashier's, manager's or certified checks or other similar instruments issued in blank or payable to cash, bearer or numbered account shall take such measure(s) as may be necessary to ensure that said instruments are not being used / resorted to by the buyer or depositor in furtherance of an ML activity;
(v) The deposit of said instruments shall be subject to the same requirements of scrutiny applicable to cash deposits; and
(vi) Transactions involving said instruments should be accordingly reported to the AMLC if there is reasonable ground to suspect that said transactions are being used to launder funds of illegitimate origin.

m. Second-endorsed checks. A covered person shall enforce stricter guidelines in the acceptance of second-endorsed checks including the application of enhanced due diligence to ensure that they are not being used as instruments for money laundering or other illegal activities.

For this purpose, a covered person shall limit the acceptance of second-endorsed checks from properly identified customers and only after establishing that the nature of the business of said customer justifies, or at least makes practical, the deposit of second-endorsed check. In case of isolated transactions involving deposits of second-endorsed checks by customer who are not engaged in trade or business, the true and full identity of the first endorser shall be established and the record of the identification shall also be kept for five (5) years.

n. *Foreign exchange dealers/money changers/ remittance and transfer companies.* A covered person shall require its customers who are remittance and transfer companies, foreign exchange dealers and money changers to submit proof of registration with the Bangko Sentral as part of their customer identification document, and shall only deal with these entities if they are duly registered as such. Also, these customers shall be required to use company accounts for their remitting, foreign exchange dealing and money changing business.

Remittance and transfer companies, foreign exchange dealers and money changers presenting greater risk shall be subject to enhanced due diligence, which includes, among others, requiring proof of registration with the AMLC, reviewing and assessing their AML/CFT program to have reasonable assurance on their AML compliance, obtaining additional information and securing senior management approval for establishing business relationship.

o. *Other high risk customer.* A customer from a foreign jurisdiction that is recognized as having inadequate internationally accepted AML standards, or presents greater risk for ML/TF or its associated unlawful activities, shall be subject to enhanced customer due diligence. Information relative to these are available from publicly available information such as the websites of FATF, FATF Style Regional Bodies (FSRB) like the Asia Pacific Group on Money Laundering and the Egmont Group, national authorities like the OFAC of the U.S. Department of the Treasury, or other reliable third parties such as regulators or exchanges, which shall be a component of a covered person's customer identification process.

p. *Shell company/shell bank/bearer share entities.* A covered person shall undertake banking relationship with a shell company with extreme caution and always apply enhanced due diligence on both the entity and its beneficial owner/s.

No shell bank shall be allowed to operate or be established in the Philippines. Covered persons shall refuse to deal, enter into, or continue, correspondent banking relationship with shell banks. They shall likewise guard against establishing relations with foreign financial institutions that permit their accounts to be used by shell banks.

Bearer share entities refer to those juridical entities where the ownership is accorded to those who possess the bearer share certificate. A covered person dealing with bearer share entities shall conduct enhanced due diligence on said entities and their existing stockholders and/or beneficial owners at the time of opening of the account. These entities shall be subject to ongoing monitoring at all times and the list of stockholders and/or beneficial owners shall be updated within thirty (30) days after every transfer of ownership and the appropriate enhanced due diligence shall be applied to the new stockholders and/or beneficial owners.

q. *Numbered accounts.* No peso and foreign currency non-checking numbered accounts shall be allowed without establishing the true and full identity and existence of customers and applying enhanced due diligence in accordance with Subsec. X806.1 (b) /4806Q.1.(b).

Peso and foreign currency non-checking numbered accounts existing prior to 17 October 2001 shall continue to exist but the covered person shall establish the true and full identity and existence of the beneficial owners of such accounts and apply enhanced due diligence in accordance with Subsec. X806.1 (b)/ 4806Q.1 (b).

r. *Prohibited accounts.* A covered person shall maintain accounts only in the true and full name of the account owner. The provisions of existing law to the contrary notwithstanding, anonymous accounts, accounts under fictitious names, numbered checking accounts and all other similar accounts shall be absolutely prohibited."

Section 7. Subsection X806.3/4806Q.3 shall be amended to read, as follows:

"**Subsection X806.3/4806Q.3** ***On-going monitoring of customers, accounts and transactions.***

a. Covered persons shall ensure that they have established the true and full identity of their customers and shall, on the basis of materiality and risk, update, no later than once every three (3) years, all customer identification information and documents, including photo, required to be obtained under the AMLA, as amended, its RIRR and this Part, unless enhanced ongoing monitoring is warranted.

Covered persons shall establish a system that will enable them to understand the normal and reasonable account or business activity of customers to ensure that the customers' accounts and transactions are consistent with their knowledge of the customers, and the latter's commercial activities, risk profile, and source of funds and detect unusual or suspicious patterns of account activity. Thus, a risk-and-materiality-based on-going monitoring of customer's accounts and transactions should be part of a covered person's customer due diligence.

b. Enhanced due diligence. Covered persons shall examine the background and purpose of all complex, unusually large transactions, all unusual patterns of transactions, which have no apparent economic or lawful purpose, and other transactions that may be considered suspicious. Covered persons shall apply enhanced due diligence on the customer in accordance with Subsec. X806.1 (b)/4806Q.1 (b) if they acquire information in the course of customer account or transaction monitoring that:

(1) Raises doubt as to the accuracy of any information or document provided or the ownership of the entity;
(2) Justifies reclassification of the customer from low or normal risk to high risk pursuant to this Part or by their own criteria; or
(3) Indicates that any of the circumstances for the filing of a suspicious transaction report exists such as but not limited to the following:

(a) xxx;
(b) xxx;
(c) xxx; or
(d) xxx.

If the covered person:

(1) fails to satisfactorily complete the enhanced due diligence procedures; or
(2) reasonably believes that performing the enhanced due diligence process will tip-off the customer,

it shall file a suspicious transaction report, and closely monitor the account and review the business relationship."

Section 8. Subsection X806.4/4806Q.4 on non-discrimination against certain types of customers shall be incorporated, to read as follows:

"**Subsection X806.4/4806Q.4** ***Non-discrimination against certain types of customers.*** The provisions of this Part shall not be construed or implemented in a manner that will discriminate against certain customer types, such as PEPs, as well as their relatives, or against a certain religion, race or ethnic origin, or such other attributes or profiles when used as the only basis to deny these persons access to the covered person's services. In this regard, covered persons shall have appropriate policies and procedures to ensure non-discrimination against certain customer types when implementing AML/CFT regulations. Covered persons who will commit said discriminatory act shall be subject to appropriate sanctions provided under existing laws and regulations."

Section 9. Section X807/4807Q, Subsections X807.1 to X807.3/4807Q.1 to 4807Q.3 and Subsection X807.6/4807Q.6 shall be amended to read as follows:

"**Section X807/4807Q Covered and Suspicious Transaction Reporting.** Covered persons shall report to the AMLC all covered and suspicious transactions within five

(5) working days, unless the AMLC prescribes a different period not exceeding fifteen (15) working days, from the occurrence thereof.

For suspicious transactions, "occurrence" refers to the date of determination of the suspicious nature of the transaction, which determination should be made not exceeding ten (10) calendar days from the date of transaction. However, if the transaction is in any way related to, or the person transacting is involved in or connected to, an unlawful activity or money laundering offense, the ten (10)-day period for determination shall be reckoned from the date the covered person knew or should have known the suspicious transaction indicator.

Should a transaction be determined to be both a covered and suspicious transaction, the covered person shall be required to report the same as a suspicious transaction.

Covered persons shall ensure the accuracy and completeness of covered and suspicious transaction report, which shall be filed in the forms prescribed by the AMLC and submitted in a secured manner to the AMLC in electronic form.

Subsection X807.1/4807Q.1 ***Deferred reporting of certain covered transactions.*** Covered persons shall refer to the issuances of the AMLC from time to time on transactions that are considered as "non-cash, no/low risk covered transactions", hence subject to deferred reporting.

The Bangko Sentral may consider other transactions as "no/low risk covered transactions" and propose to the AMLC that they be likewise subject to deferred reporting by covered persons.

Subsection X807.2/4807Q.2 ***Electronic monitoring systems for AML/CFT.*** Covered persons required under Subsec. X805.3 (a)/4805Q.3 (a) to have an electronic monitoring system for AML/CFT should ensure that the system, at a minimum, shall detect and raise to the covered person's attention, transaction and/or accounts that qualify either as covered transaction (CT) or suspicious transaction (ST) as herein defined. The covered person shall endeavor to interface the electronic monitoring system with the systems of its branches, subsidiaries and affiliates, if any, for group-wide AML/CFT monitoring.

The system must have at least the following automated functionalities:

a. Covered and xxx
b. xxx
c. xxx
d. Can generate all the CTRs of the covered person accurately and completely with all the mandatory field properly filled up;
e. xxx;
f. xxx;
g. xxx.

Covered persons with existing electronic system of flagging and monitoring transactions already in place shall ensure that their existing system is updated to be fully compliant with functionalities as those required herein.

Subsection X807.3/4807Q.3 ***Manual monitoring.*** Covered persons which are not required, under this Part, to have an electronic system of flagging and monitoring transactions shall ensure that they have the means of flagging and monitoring the transactions mentioned in Subsec. X807.2/4807Q.2. They shall maintain xxx."

"**Subsection X807.6/4807Q.6** ***Confidentiality provision.*** When reporting CTs and STs to the AMLC, covered persons, their directors, officers and employees, are prohibited from communicating, directly or indirectly, in any manner or by any means, to any person or entity, or the media, the fact that a covered or suspicious transaction report was made, the contents thereof, or any other information in relation thereto. Any information about such reporting shall not be published or aired, in any manner or form, by the mass media, or through electronic mail, or other similar devices. In case of violation thereof, the concerned director, officer and employee of the covered person shall be criminally liable."

Section 10. Appendices 6, Q-3 and T-3 shall be amended by deleting the STRs and CTRs.

Section 11. Section X808/4808Q and Subsections X808.1/4808Q.1, X808.2/4808Q.2, and X808.4/4808Q.4 shall be amended to read as follows:

"**Section X808/4808Q Record Keeping.** All customer identification records of covered persons shall be maintained and safely stored as long as the account exists. All transaction records and documents of covered persons shall be maintained and safely stored for five (5) years from the date of transaction.

Said records and files xxx in Subsec. X806.2 (b) for xxx. Covered persons shall undertake the necessary adequate security measures to ensure the confidentiality of such file. Covered persons shall prepare and maintain xxx, and/or the courts to establish an audit trail for money laundering.

Subsection X808.1/4808Q.1 ***Closed accounts.*** Covered persons shall maintain and safely store all records of customer identification, and transaction documents for at least five (5) years from the date the account was closed.

Subsection X808.2/4808Q.2 ***Retention of records where the account or customer is the subject of a case.*** If a money laundering case has been filed in court involving the account or customer, records must be retained and safely kept beyond the five (5)-year retention period, until it is officially confirmed by the AMLC Secretariat that the case has been resolved, decided or terminated with finality."

"**Subsection X808.4/4808Q.4** ***Form of records***. Covered persons shall retain all records as originals or in such forms as are admissible in court pursuant to existing

laws, such as the E-Commerce Act and its implementing rules and regulations, and the applicable rules promulgated by the Supreme Court.

Covered persons shall, likewise, keep the electronic copies of all CTRs and STRs for at least five (5) years from the dates of submission to the AMLC.

For low risk customers, it is sufficient that covered persons shall maintain and store, in whatever form, a record of customer information and transactions."

Section 12. Section X810/4810Q shall be amended to read as follows:

"Section X810/4810Q Bangko Sentral Authority to Check Compliance with the AMLA, as amended. In the course of a periodic or special examination, the Bangko Sentral may inquire into or examine bank accounts or investments, including customer identification, account opening, and transaction documents, for the purpose of checking compliance by covered persons under its supervision or regulation with the requirements of the AMLA, as amended, its RIRR, other AMLC issuances and this Part.

The Bangko Sentral xxx

In the course of xxx, the covered person, its officers and employees, and the Bangko Sentral xxx."

Section 13. The first four paragraphs of Section X811/4811Q shall be amended and a new paragraph on escalation of enforcement action is incorporated before the provisions on monetary guidelines, to read as follows:

"Section X811/4811Q Sanctions and Penalties. In line with the objective of ensuring that covered persons maintain high AML/CFT standards in order to protect its safety and soundness as well as protecting the integrity of the national banking and financial system, violation of this Part shall constitute a major violation subject to the following enforcement actions xxx and whenever applicable:

a. Written reprimand;
b. Restriction on certain licenses/product, as appropriate;
c. Suspension or removal from the office they are currently holding; and/or
d. Disqualification from holding any position in any covered institution.

In addition xxx.

Enforcement action shall be imposed on the basis of the overall assessment of the covered person's AML risk management system. Whenever a covered person's AML compliance xxx.

To implement xxx

1. xxx
2. An AML composite rating of 2 or 1 will require submission by the covered person to the appropriate department of the SES, of a written action plan xxx.

   The appropriate department of the SES shall assess the viability of the plan and shall monitor the covered person's performance.

   In the event xxx, the appropriate department of the SES shall recommend appropriate enforcement action on the covered person and xxx.

3. An AML rating of 1 xxx. For this reason, prompt corrective action shall be initiated on the covered person.

Escalation of enforcement action. In cases of heightened AML/CFT supervisory concern as reflected in the overall AML risk rating over a certain period of time, the Bangko Sentral shall impose escalated enforcement action which shall include corrective action, sanction and/or additional supervisory enforcement action, consistent with Section X009/4009Q on supervisory enforcement policy."

Section 14. The following Sections/Subsections/provisions shall be retained except that all reference to "covered institution" or "covered institutions" shall be replaced with "covered person" or "covered persons", respectively:

a. Sections X804/4804Q and X809/4809Q;
b. Subsection X807.4/4807Q.4, X807.5/4807Q.5 and X808.3/4808Q.3;
c. Provisions under monetary penalty guidelines in Section X811/4811Q; and
d. Section 4691S, Subsec. 4691S.9 and Section 4104N.

Section 15. Separability Clause. If any provision, sections of this Circular, or its application to any person or circumstance is held invalid, the other provisions or sections of this Circular, and the application of such provision or section to other persons or circumstance shall not be affected thereby.

Section 16. Effectivity. This Circular shall take effect fifteen (15) calendar days after is publication either in the Official Gazette or in a newspaper of general circulation in the Philippines.

FOR THE MONETARY BOARD:

AMANDO M. TETANGCO, JR.
Governor

15 March 2017